Les signaux

Table des matiéres

I) SYNCHRONISATION DES PROCESSUS

Sous UNIX, les processus disposent d'espace mémoire indépendants assurant la sécurité mutuelle des codes et des données. Néanmoins ce système interdit toute possibilité de synchronisation entre processus et, bien entendu, de communications entre eux.
Néanmoins, UNIX implémente certains dispositifs qui permettent de réaliser la coordination entre les processus au cours de leurs exécutions.

1) Les signaux

a) Généralités

Des événements extérieurs ou intérieurs au processus peuvent survenir à tout moment et provoquer une interruption de l'exécution du processus en cours. Ces événements peuvent être d'origine "physique" (coupure de courant, lecteur non prêt, etc.) ou logique.
Lors de la réception d'une interruption, le noyau reconnaît l'origine de celle-ci, sauve le contexte du processus actuel et provoque l'exécution d'une routine appropriée ***handler***. Le mécanisme est semblable à celui des interruptions sous DOS.
La technique des signaux est utilisée par le noyau pour prévenir un processus de l'existence d'un événement extérieur le concernant. Elle correspond à l'utilisation, dans d'autres systèmes d'exploitation, du principe des interruptions logicielles. L'origine d'un signal peut être variée, elle peut être d'origine matérielle, système ou logicielle. Ce peut être :

- ✓ la fin d'exécution d'un processus fils
- ✓ l'utilisation d'une instruction illégale dans le programme
- ✓ la réception d'un signal d'alarme
- ✓ une demande d'arrêt de la part du processus
- ✓ etc.

Le noyau prévoit une réaction par défaut à chaque signal (routine ***handler***). Cette réaction est en général d'arrêter le processus recevant ce signal, mais le comportement du processus à la réception d'un signal peut être configurable. Le processus peut ainsi se prémunir contre l'effet de certains signaux.

b) Les signaux

Les différents signaux sont représentés par des numéros auxquels sont associés des noms symboliques utilisés par les compilateurs.

Nom	***N°***	***Rôle***	***Core***	***Ignoré***
SIGHUP	1	émis au processus attaché à un terminal, lorsque celui-ci est déconnecté (HangUP)		
SIGINT	2	émis au processus attaché au terminal sur lequel on frappe <DEL> ou <SUPPR>		
SIGQUIT	3	idem pour la touche <QUIT>	**X**	
SIGILL	4	envoyé au processus qui tente d'exécuter une instruction illégale	**X**	
SIGTRAP	5	envoyé après chaque instruction. Utilisé par les programmes de mise au point	**X**	
SIGIOT	6	émis en cas de problème matériel	**X**	
SIGEMT	7	utilise pour les calculs en virgule flottante		
SIGFPE	8	erreur sur les flottants	**X**	
SIGKILL	9	émis pour tuer le processus		
SIGBUS	10	émis en cas d'erreur sur le bus	**X**	
SIGSEGV	11	émis lors d'une violation de mémoire	**X**	
SIGSYS	12	émis lors d'une erreur dans les paramètres transmis à une primitive	**X**	
SIGPIPE	13	émis lors de l'écriture dans un pipe sans lecteur		
SIGALRM	14	signal associé à l'horloge système		
SIGTERM	15	signal de fin normale d'un processus		
SIGUSR1	16	offert aux utilisateurs		
SIGUSR2	17	idem		
SIGCHLD	18	émis vers le père à la mort du fils		**X**
SIGPWR	19	émis lors d'une coupure de courant		**X**
SIGPOLL	22	événement sélectionné		**X**

core : X, ces signaux génèrent un fichier core
Certains signaux génèrent la production d'une image du contexte du processus lors de son interruption. Cette image est appelée core. Un message "core dumped" est alors envoyé sur l'écran par le système : et un fichier core est créé dans le répertoire de travail. Il peut être lu avec certains outils (débuggeur) pour essayer de comprendre ce qui a pu générer l'interruption.

Ignoré : X, ces signaux sont ignorés par défaut
Chaque système UNIX soutient un nombre différent de signaux. De plus les numéros n'ont pas la même signification. Il n'y a que les constantes prédéfinies qui soient portables

c) Fonctionnement d'un signal :

Envoi d'un signal :

Un signal peut être envoyé par le noyau ou un processus. Ce signal est mémorisé dans un champ de la table proc du processus récepteur (on dit que c'est un signal pendant) : chaque signal active un bit particulier de ce champ.

Lorsque le processus récepteur doit être activé ou lorsqu'il réalise un appel système, le scheduler lit ce champ est fait exécuter les routines correspondantes aux différents bits de signaux activés (le signal est dit délivré).

Le moment entre l'émission du signal et sa prise en compte par le processus est donc indéterminé.

Sous System V Release 4 un signal peut être bloqué : sa prise en compte est différée jusqu'à ce que le signal ne soit plus bloqué.

Réception d'un signal :

En règle générale, la réception d'un signal provoque l'arrêt de l'exécution d'un processus avec éventuellement génération d'une image mémoire core et se traduit par l'exécution de la fonction handler associée.

d) Fonctions de gestions des signaux :

La primitive ***kill()*** envoie un signal à un processus . Elle prend en paramètre l'identificateur du processus destinataire et le numéro du signal. Si la valeur PID=0 est utilisée, le signal est envoyé à tous les processus du groupe.

```
#include <signal.h>
int kill (int pid, int sig);
```

Explication des paramètres :

✓ int pid : numéro du processus où sera envoyé le signal. Ce numéro peut avoir quatre groupe de valeurs

- Une valeur ***n*** positive enverra le signal au processus de pid "n"
- La valeur ***0*** enverra le signal à tous les processus du même groupe que le processus appelant
- La valeur ***–1*** enverra le signal à tous les processus tournant sur la machine (sauf le premier "*init*") par ordre de pid décroissant
- Une valeur ***n*** négative autre que ***–1*** enverra le signal à tous les processus du même groupe que le processus de pid "-n"

✓ int sig : numéro du signal à envoyer. La valeur ***0*** est utilisée pour vérifier que le processus existe.

Valeur renvoyée (int) : 0

La fonction ***signal()*** permet de prémunir un processus contre l'effet principal de la réception d'un signal quelconque qui est d'arrêter son exécution. Cette fonction ira installer dans une zone particulière correspondant au signal attendu une adresse de déroutement (fonction).

```
#include <signal.h>
int signal (int sig, void (*pt_fonc)(int));
```

Explication des paramètres :

✓ int sig : numéro du signal devant être reçu

✓ void (*pt_fonc)(int) : référence (adresse) de la fonction qui sera exécutée lors de la réception dudit signal. Cette fonction, à charge du programmeur, doit impérativement être prévue pour recevoir un ***int*** (qui sera, dans la fonction, le signal reçu) et ne doit rien renvoyer (***void***). Deux valeurs particulières peuvent êtres utilisées pour ce paramètre :

- SIG_IGN : le signal est purement et simplement ignoré (mais il est quand même acquitté). Ce paramètre est utile si la réception d'un signal ne donne pas lieu à l'appel d'une fonction particulière
- SIG_DFL : restitue au processus son comportement par défaut (mourir)

Valeur renvoyée (int) : Valeur précédente de déroutement.

Le signal 9 (SIGKILL) ne peut pas être ignoré ni détourné.

Remarque **spécifique** à l'environnement **System V** :
Lors de la réception d'un signal, la fonction préalablement chargée par la primitive ***signal()*** est alors exécutée. Mais dans le même temps, le comportement par défaut du processus est restauré. Ce qui signifie que lors de la réception d'un nouveau signal, le processus aura retrouvé son comportement original et se terminera.
Pour avoir un aspect permanent, une fonction prévue à la réception d'un signal doit procéder à une réinstallation de son propre code au moyen de la même primitive ***signal()***.

Exemple :

```
#include <stdio.h>
#include <unistd.h>
#include <signal.h>

void ex_program(int sig);

int main() {
 (void) signal(SIGINT, ex_program);

 while(1)
printf("Dormir .. ZZZzzzz ....\n"), sleep(1);

 return 0;
}

void ex_program(int sig) {
 printf("C'est l'heure ... !!! - Capture du signal: %d ... !!\n", sig);
 (void) signal(SIGINT, SIG_DFL);
}
```

Cette remarque ne s'applique pas à l'environnement **BSD,** un signal détourné une fois le reste en permanence ou jusqu'à ce que son comportement par défaut soit restauré. Il est interressant de noter que la norme **POSIX** qui tend à se mettre en place un peu partout correspond, pour la primitive ***signal()***, à cet environnement.

la primitive ***pause()*** suspend l'exécution du processus qui l'invoque jusqu'à l'arrivée d'un signal, quel qu'il soit. Bien entendu, si le processus n'a pas, au préalable, détourné le signal arrivant, ce processus ne se réveillera que pour mourir.

```
#include <unistd.h>
int pause (void);
```

la primitive ***alarm()*** duplique son code lors de l'appel (tout comme la primitive ***fork()***) mais le code dupliqué n'est pas accessible au programmeur

✓ Le code père (qui a lancé la primitive) rend immédiatement la main (et peut donc faire autre-chose

✓ Le code fils (qui vient d'être généré) attendra un certain temps et, lorsque ce temps sera écoulé, enverra au processus père (processus qui a lancé la primitive) un signal SIGALRM , puis se terminera proprement.

```
#include <unistd.h>
int alarm (int sec);
```

Explication des paramètres :

✓ int sec : temps d'attente du fils

Cette primitive peut-être utilisée lorsqu'on veut prévenir un processus de manière automatique (temps écoulé, etc.)

Remarque : lancer une seconde fois cette primitive alors que le temps de la première n'est pas encore écoulé annule le premier appel.

e) Gestion du signal SIGCHLD :

Ce signal est envoyé par tout processus fils à son processus père lorsqu'il meurt. Il faut dans certains cas réaliser une bonne gestion de la réception de ce signal.

Rappel : Il est possible que le processus père, après avoir créé un processus fils, ait continué son exécution sans attendre la terminaison de son fils. Un processus fils restera dans l'état de processus "zombie" aussi longtemps que son père n'aura pas consulté son code de retour.

L'indicateur d'arrivée du signal SIGCHLD est positionné dans le bloc de contrôle des signaux du processus père dès qu'un de ses fils s'est terminé et le reste aussi longtemps que le code de retour d'un de ses fils n'a pas été consulté par l'intermédiaire de la primitive ***wait()***. Il est par conséquent essentiel de gérer correctement la terminaison des processus fils afin de ne pas saturer la table des processus avec des processus zombies. C'est un appel à la primitive ***wait()*** qui bascule l'état du bit de contrôle du signal SIGCHLD, à la différence des autres signaux.

Pour assurer une bonne gestion de la mort des processus fils, et donc d'éviter la création de processus zombies, il est préférable d'utiliser la primitive ***waitpid()***, qui est une extension optimisée de la primitive ***wait()***.

2) LES VERROUS

a) Généralités :

Du fait de l'environnement Multi-Utilisateurs, il est possible que plusieurs d'entre eux tentent d'accéder en même temps à une même ressource (fichier ou imprimante...).
L'accès à un fichier est à considérer comme un accès à une ressource critique dans la mesure où des accès non maîtrisés rendent le contenu d'un fichier aléatoire. Il faut donc mettre au point des systèmes permettant de contrôler ces accès : les verrous sont une première réponse mise à la disposition des programmeurs.
Il faut se rappeler que sous Unix tout pouvant être considéré comme un fichier, la technique des verrous est donc générale.

b) Types de verrous :

UNIX propose diverses possibilités de verrous : il y a les verrous externes, devenus obsolètes, et les verrous intégrés à l'objet à verrouiller. D'autre part, un verrou peut agir sur la totalité du fichier ou seulement sur une partie de celui-ci.

Enfin un verrou peut être :

✓ **impératif** : Il interdit alors effectivement la réalisation de certaines opérations d'E/S. C'est le verrou le plus efficace mais il alourdit le travail du noyau.

✓ **consultatif** : Il faut alors que les processus testent l'existence du verrou. S'ils ne le font pas ils peuvent réaliser les E/S souhaitées mais le verrou est alors inutile.

✓ **partagé/exclusif** : Un verrou partagé (en lecture) est compatible avec des verrous du même type : il vise essentiellement, en lecture, à interdire toute modification du fichier et à empêcher la pose d'un verrou exclusif en écriture.

L'utilisation non contrôlée de verrou peut conduire à des situations de blocage lorsque deux processus ont chacun posé un verrou exclusif bloquant l'autre processus.
Un verrou en lecture ne peut être posé que s'il n'existe pas de verrou en écriture sur le fichier. De même un verrou en écriture ne peut être posé que s'il n'existe aucun verrou sur le fichier.

c) Gestions des verrous par le système :

Les manipulations de verrous se font par l'intermédiaire de la primitive ***fcntl()***. Le système gère une table des verrous au sein du noyau.
Les différents verrous posés sur un fichier donné sont chaînés. Une entrée dans la table des verrous contient les informations suivantes :

✓ Type de verrou (écriture/lecture)

✓ Caractéristiques de la zone verrouillée (début et longueur)

✓ Un pointeur sur l'entrée, dans la table des processus, du processus poseur du verrou

Les pointeurs de chaînage des verrous.La structure ***flock***, définie dans ***fcntl.h***, sert à la réalisation par la primitive ***fcntl()*** des diverses opérations sur les verrous :

```
struct flock {
    short l_type;               /* type de verrou */
    short l_whence;         /* position absolue début du verrou */
    long l_start;               /* position relative début du verrou */
    long l_len;                 /* longueur de la zone verrouillée */
    short l_pid;                /* processus propriétaire */
}
```

Explication des éléments :

- ✓ short l-type : type de verrou posé
  - F_RDLCK : verrou partagé (en lecture)
  - F_WRLCK : verrou exclusif (en écriture)
  - F_UNLCK : absence de verrou
- ✓ short l_whence : portée du verrou selon trois paramètres :
  - 0 le début de la zone verrouillée est au début du fichier
  - 1 la zone verrouillée commence à la position courante
  - 2 : la zone verrouillée commence à la fin du fichier
- ✓ long l_start : position de départ relative au champ ***l_whence*** où sera posé le verrou
- ✓ long l_len : longueur de la zone verrouillée. Une valeur spéciale ***0*** indique que le verrou sera posé jusqu'à la fin du fichier
- ✓ short l_pid : numéro du propriétaire du verrou
- ✓ e type de verrou posé

d) Manipulation des verrous :

La primitive ***fcntl()*** permet de réaliser une opération de verrouillage sur un fichier particulier.

```
#include <fcntl.h>
int fcntl (int desc, int op, struct flock *pt_verrou);
```

Explication des paramètres :

- ✓ int desc : descripteur du fichier concerné
- ✓ int op : opération à effectuer. Celles-ci sont au nombre de 3 :
  - F_GETLK : lecture des caractéristiques d'un verrou existant
  - F_SETLK : pose ou changement de verrou en mode non bloquant
  - F_SETLKW : pose ou changement de verrou en mode bloquant
- ✓ struct flock *pt_verrou : pointeur vers une variable de type ***struct flock***. Celle-ci devra avoir été préalablement remplie.

La pose d'un verrou en lecture suppose le descripteur ouvert en lecture (idem pour une écriture).
La fermeture d'un descripteur par un processus implique la levée de tous les verrous posés par ce processus sur le fichier correspondant au descripteur.

Exemple :

```
#include <stdio.h>
#include <errno.h>
#include <fcntl.h>

main (int argc, char *argv[ ])
{
        int  m, d;
        char c;
        stuct flock verrou;

        d=open("fic ", O_RDWR);
        verrou.l_type=F_WRLCK;
        verrou.l_whence=0
        verrou.l_start=0
        verrou.l_len=0;
        while (fcntl (d, F_SETLK, &verrou) == (-1) && (errno == EACCES || errno == EAGAIN))
        {
                perror("Pose de verrou impossible\n");
                sleep (5);
        }
        printf ("Verrou posé\n");
        while ((m=read (d, &c, 1)) != 0)
        {
                if (c == '# ')
                {
                        lseek (d, -1L, 1);
                        sleep (1);
                        write (d, argv[1], 1);
                        return(0);
                }
                if (m== 0)
                        printf (" Pas d'occurrence du caractère '#'\n");
        }
}
```

3) Dispositif de scrutation

On est parfois amené à vouloir qu'un processus récupère des informations sur un ou plusieurs périphériques du système, via des descripteurs de fichier. La plupart du temps les opérations de lecture et écriture sur ces dispositifs étant bloquantes, il est difficile d'assurer la lecture de tous ces descripteurs dans des délais satisfaisant ce qui est pénalisant en termes de performances.

Il est donc souhaitable que l'on puisse utiliser des primitives permettant au processus,

- ✓ soit de lire alternativement en mode non bloquant sur chaque descripteur
- ✓ soit d'être averti par le système lorsqu'une lecture doit être réalisée sur un descripteur.

La primitive poll () :La structure ***pollfd***, définie dans ***sys/poll.h***, permet la réalisation par la primitive ***poll()*** de multiplexage par un processus

```
struct pollfd {
    int fd;                    /* descripteur du fichier à scruter */
    short events;              /* événements attendu sur le fichier */
    short revents;             /* événement survenus sur le fichier */
}
```

Explication des éléments :

- ✓ int fd : descripteur du fichier à interroger
- ✓ short event : champ contenant les évènements à scruter
- ✓ short revents : champ contenant les évènements survenus

La primitive ***poll()*** permet la réalisation de multiplexage par un processus.

```
#include <sys/poll.h>
int poll (struct pollfd *pt_tabpoll, int nbelem, int temps);
```

Explication des paramètres :

- ✓ struct pollfd *pt_tabpoll : pointeur vers un tableau de variables de type ***struct pollfd***. Chacune des variables du tableau aura été préalablement remplie.
- ✓ int nbelem : Nombre d'éléments contenus dans le tableau
- ✓ int temps : durée de la scrutation en millisecondes

Valeur renvoyée (int) : nombre de fichiers ayant reçu au moins un évènement attendu (champ ***revents*** non nul).

Les événements sont obtenus comme combinaison des événements suivants :

- ✓ POLLIN : lecture possible de données autres que *hautement prioritaire*
- ✓ POLLRDNORM : lecture possible de données *normales*
- ✓ POLLRDBAND : lecture possible de données *prioritaires*
- ✓ POLLPRI : lecture possible de données *hautement prioritaires*
- ✓ POLLOUT : écriture possible de données
- ✓ POLLWRNORM : *idem* POLLOUT
- ✓ POLLWRBAND : écriture possible de données *prioritaires*
- ✓ POLLERR (champ ***revents*** uniquement) : une erreur est intervenue
- ✓ POLLHUP (champ ***revents*** uniquement) : coupure de ligne
- ✓ POLLINVAL (champ ***revents*** uniquement) : le fichier spécifié n'est pas ouvert

a) Entrées-Sorties asynchrones :

Les processus peuvent demander au noyau de les avertir lorsqu'une lecture ou une écriture est réalisable sur un fichier. Ils recevront alors le signal SIGIO.
Pour pouvoir réaliser cela il faut réaliser les opérations suivantes :

- ✓ Créer un handler pour traiter la réception du signal SIGIO.
- ✓ Armer la réception du signal pour le processus ou le groupe de processus, souhaité. Cette action est réalisée par la fonction fcntl ().
- ✓ Positionner l'option asynchrone pour le processus, en utilisant la primitive ***fcntl()***.

Exemple :

```
#include < signal.h>
#include < stdio.h>

void r_sigio ()                                  /* routine à associer au signal SIGIO */
{
        char buf[80];
        int nb;                                  /* nombre d'octets */

        nb=read(0, buf, 80);
        buf[nb]=0;                               /* transformation en chaîne de caractères */
        printf("le message reçu est : '%s'\n", buf);
}

int main ()
{
        signal(SIGIO, r_sigio);                  /* détournement signal */
        fcntl (0, F_SETOWN, getpid ());

        fcntl (0, F_SETFL, FASYNC);              /* mode E/S asynchrones */

        i=0;
        while (1)                                /* boucle interrompue par SIGIO */
                printf (" i=%d\n", i++);
}
```